

**国家电网公司**

**XXXX信息系统概要设计**

**(项目编号： )**

**V2.0**

**(征求意见稿)**

**XXX单位/部门**

**XXXX年XX月**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 文件编号： | | 生效日期： | | 受控编号： | |
| 密级： | | 版次：Ver | | 修改状态： | |
| 总页数 |  | 正文 |  | 附录 |  |
| 架构师： | | 审核： | | 批准： | |

文档修改记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 日期 | 修改页 | 作者 | 批准人 |
| V1.0 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

[1概述 1](#_Toc358153845)

[1.1编写目的 1](#_Toc358153846)

[1.2术语与定义 1](#_Toc358153847)

[1.3参考资料 1](#_Toc358153848)

[2标准和规范 1](#_Toc358153849)

[2.1引用的标准和规范 1](#_Toc358153850)

[2.2拟制定的标准和规范 2](#_Toc358153851)

[3系统总体框架 2](#_Toc358153852)

[3.1项目概览 2](#_Toc358153853)

[3.2总体设计原则 2](#_Toc358153854)

[3.3总体技术路线 3](#_Toc358153855)

[3.4架构遵从 3](#_Toc358153856)

[4业务能力视图 5](#_Toc358153857)

[4.1业务功能 5](#_Toc358153858)

[4.2业务流程 6](#_Toc358153859)

[5功能视图 6](#_Toc358153860)

[5.1功能视图 6](#_Toc358153861)

[5.2功能清单 6](#_Toc358153862)

[6系统数据视图 6](#_Toc358153863)

[6.1概念数据模型 6](#_Toc358153864)

[6.2逻辑数据模型 7](#_Toc358153865)

[6.3数据分类 8](#_Toc358153866)

[6.4数据流转 9](#_Toc358153867)

[6.5数据存储与分布 10](#_Toc358153868)

[7系统组件视图 10](#_Toc358153869)

[7.1系统逻辑分层 10](#_Toc358153870)

[7.2组件关联设计 11](#_Toc358153871)

[7.3功能组件设计 12](#_Toc358153872)

[7.4公共组件设计 13](#_Toc358153873)

[8系统集成视图 16](#_Toc358153874)

[8.1总体集成 16](#_Toc358153875)

[8.2集成场景 16](#_Toc358153876)

[8.3集成设计 17](#_Toc358153877)

[9系统逻辑部署视图 21](#_Toc358153878)

[9.1部署单元设计 21](#_Toc358153879)

[9.2部署节点设计 22](#_Toc358153880)

[10系统物理部署视图 23](#_Toc358153881)

[10.1部署拓扑 23](#_Toc358153882)

[10.2容量规划 23](#_Toc358153883)

[10.3硬件环境设计 23](#_Toc358153884)

[10.4软件环境设计 24](#_Toc358153885)

[11系统灾备视图 25](#_Toc358153886)

[11.1关键技术选择 25](#_Toc358153887)

[11.2灾备策略设计 25](#_Toc358153888)

[11.3灾备架构设计 25](#_Toc358153889)

[11.4灾备设备配置 26](#_Toc358153890)

[12系统安全视图 27](#_Toc358153891)

[12.1总体安全视图 27](#_Toc358153892)

[12.2应用安全 28](#_Toc358153893)

[12.2数据安全 29](#_Toc358153894)

[12.3主机安全 30](#_Toc358153895)

[12.4网络安全 30](#_Toc358153896)

[12.5终端安全 31](#_Toc358153897)

[12.6其他 31](#_Toc358153898)

[13附录 31](#_Toc358153899)

[13.1系统组件视图 33](#_Toc358153900)

[13.2逻辑数据实体分项定义 34](#_Toc358153901)

[13.3系统安全设计子方案 34](#_Toc358153902)

图 表

[图1 <网上营业厅>功能层级图 6](#_Toc357620052)

[图2 跨网省调动管理流程 7](#_Toc357620053)

[图3 设备主数据维护\_非项目新增 8](#_Toc357620054)

[图4 <网上营业厅>功能层级图 9](#_Toc357620055)

[图5 概念数据模型 11](#_Toc357620056)

[图6 数据模型 12](#_Toc357620057)

[图7 数据流转图 13](#_Toc357620058)

[图8 系统逻辑分层图 15](#_Toc357620059)

[图9 组件关联图 16](#_Toc357620060)

[图10 功能组件图 17](#_Toc357620061)

[图11 公共组件图 18](#_Toc357620062)

[图12 系统总体集成图 19](#_Toc357620063)

[图13 界面集成图 20](#_Toc357620064)

[图14 应用集成设计图 21](#_Toc357620065)

[图15 数据集成设计图 22](#_Toc357620066)

[图16 部署单元 24](#_Toc357620067)

[图17 部署节点 25](#_Toc357620068)

[图18 物理部署视图 26](#_Toc357620069)

[图19 灾备逻辑架构视图 29](#_Toc357620070)

# 1概述

## 1.1编写目的

*【编写说明】编写这份概要设计说明书的目的、适用范围。*

*【示例】*

*此概要设计说明文档的编写目的是为项目组后续开展详细设计、系统建设与实现、系统测试提供依据。*

## 1.2术语与定义

*【编写说明】列出本文档中所用到的术语的定义和缩写词的原词组及含义。*

*【示例】*

*1、SG-ERP总体架构：继承SG186工程八大业务应用，发展建设新一代十大业务应用；发展SG186工程集成模式，围绕业务融合场景推进多业务集成；发展SG186工程业务应用高级分析体系，建设智能决策支撑体系；继承SG186工程一体化信息平台，建设互动性更强、可视化更优的信息展现服务，实现柔性的业务应用集成服务，提升数据中心的业务连续性保障与数据资源全面管理与利用能力，提升信息网络覆盖范围与承载能力，构建集约化的基础设施服务；继承SG186工程保障体系，强化信息管控，构建扁平高效的运行维护体系。SG-ERP总体架构包含业务架构、应用架构、数据架构和技术架构四个重要组成部分。*

*2、业务架构：是信息化总体架构的起点，业务架构定义了在总体企业战略指导下希望实现的业务能力及其关系。*

*3、劳动计划管理：国家电网公司总部人资部每年年末都制定公司各单位的下一年度的招聘或调动计划方案，并对其下各单位上报各类人员的招聘计划数进行审批。年中可能存在某些单位对人力资源计划管控进行调整，比如遇上重大自然灾害或者单位重组，计划调整与计划申报流程一样，也是公司各单位上报总部人资部进行审批。*

## 1.3参考资料

*【编写说明】列出参考资料的作者、标题、编号、发表日期、出版单位或资料来源等信息。*

*【示例】*

*1、国家电网公司 “十二五”人力资源信息化发展规划*

*2、关于开展人力资源管理信息系统完善提升工作的通知*

# 2标准和规范

## 2.1引用的标准和规范

*【编写说明】列出本文档所引用的标准规范，并明确指出其所在的视图。*

表 引用的标准和规范

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 所在视图 | 标准名称 | 标准文号 |
| *1* | 系统组件视图 |  |  |
| *2* | 系统数据视图 | * *应用集成平台典型设计手册v2.6* * *SGCC\_成熟套装软件纵向贯通技术实现v2* |  |
| *3* | 系统集成视图 |  |  |
| *4* | 系统逻辑部署视图 |  |  |
| *5* | 系统物理部署视图 |  |  |
| *6* | 系统安全视图 |  |  |

## 2.2拟制定的标准和规范

*【编写说明】列出本文档所计划制定的标准规范。*

表 拟制定的标准和规范

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 标准名称 | 标准摘要 | 拟替换的标准 | 责任单位 |
| *1* | *国家电网公司主数据管理平台物料主数据标准* | *根据国家电网公司现有主数据管理体系，结合统一主数据管理的业务特点，为对物料主数据管理制定标准* | *建议替换的标准* | *必填项，明确标准编制单位* |
| *2* | *国家电网公司主数据管理平台供应商主数据标准* | *根据国家电网公司现有主数据管理体系，结合统一主数据管理的业务特点，为对供应商主数据管理制定业务标准* |  | *必填项，明确标准编制单位* |
|  |  |  |  |  |

# 3系统总体框架

## 3.1项目概览

*【编写说明】描述本项目总体概况、目标系统简述、业务目标与于业务需求映射关系、项目组成、项目边界等。*

## 3.2总体设计原则

*【编写说明】描述为达到目标系统设计所应遵循的原则。*

*在系统建设实施过程中，将遵循以下几个原则：*

*规范性原则：按照国家电网公司“SG-ERP”工程整体规划，遵循国家电网公司制定的物资编码规范等标准化设计成果，推进技术规范书、合同模板、招标文件等数据文件的标准化、结构化、规范化等工作。*

*融合适应性原则：国网公司通过SG186工程建成完备的一体化信息集成平台，系统架构的设计必须遵循融合适应的原则，系统架构中各组件的部署与集成方案应充分考虑一体化平台相关的技术政策与原则，保证建成的系统能够在国网公司一体化平台上平滑运行，实现与相关业务应用的紧密融合。*

## 3.3总体技术路线

*【编写说明】描述针对本系统拟采用的技术路线、应用类型和架构决策。*

表 架构决策

|  |  |
| --- | --- |
| 分类 | 选型原则 |
| *技术选型* | 1. *界面展现技术, 应采用成熟界面展现技术，如JSP、Flex等；* 2. *服务器开发技术，应采用业界成熟的服务器端开发技术，建议选择JavaEE技术规范（JavaEE规范采用5.0以上版本，JDK采用1.5以上版本）；* 3. *对性能有特别要求的，可以考虑选择C/C++技术。* |
| *部署模式* | 1. *仅在总部部署系统* 2. *在总部和网省分别进行部署系统* 3. *仅在网省部署系统* |
| *开发平台* | 1. *非套装软件业务应用选择Sotower或SG-UAP开发平台；* 2. *套装软件业务应用选择其本身配套的开发平台。* |
| *中间件* | *Weblogic10.2* |
| *数据库* | *事务处理数据库采用Oracle 11g，联机分析处理数据库采用Oracle 11g。* |
| *开源软件* | *选用BSD、Apache Licence 2.0、LGPL、MIT协议的开源软件* |

## 3.4架构遵从

### 3.4.1业务架构

*【编写说明】描述本系统架构对业务架构的遵从情况。此章节平台类型系统可裁剪。*

*“业务架构：业务域”应引用总体架构蓝图业务架构部分，如蓝图规划中没有相应设计，应遵循架构资产修编流程，提出架构资产修编申请。*

*“系统架构：业务功能”仅需逐一列出《软件需求规格说明书》中的第一级业务功能；“业务架构：业务职能”需参考总体架构设计蓝图的业务架构部分，说明业务功能所对应的业务职能；“遵从说明”描述系统业务功能与业务职能的遵从关系，可选项为：遵从、细化、参照（总体业务架构中没有对应项）。*

表 业务架构遵从对照

|  |  |  |
| --- | --- | --- |
| 业务域 | *营销管理* | |
| 业务职能 | | |
| 系统架构：业务功能 | 业务架构：业务职能 | 遵从说明 |
| *电量电费* | *电量电费管理* | *细化* |
|  |  |  |
| 业务流程 | | |
| 系统架构：业务流程 | 业务架构：业务流程（子流程） | 遵从说明 |
| *跨网省调动管理流程* | *员工管理流程* | *细化* |
|  |  |  |

### 3.4.2应用架构

*【编写说明】描述本系统架构对应用架构的遵从情况。此章节平台类型系统可裁剪。*

*“应用架构：应用域”，说明系统所对应实现的应用所属的应用域；*

*“应用架构：应用”，说明系统所对应实现的应用，如实现多个应用，需要逐一列出；*

*“应用架构：应用域”和“应用架构：应用”应引用总体架构蓝图应用架构部分，如蓝图规划中没有相应设计，应遵循架构资产修编流程，提出架构资产修编申请。*

*“系统架构：一级功能”仅需逐一列出《软件需求规格说明书》中的第一级系统功能；“应用架构：一级应用功能”需参考总体应用架构蓝图资产，说明系统功能所对应的应用功能；“遵从说明”描述系统功能与应用功能的遵从关系，可选项为：遵从、细化、参照（总体应用架构中没有对应项）。*

表 应用架构遵从对照

|  |  |  |
| --- | --- | --- |
| 应用架构：应用域 | *营销管理* | |
| 应用架构：应用 | *营销业务应用* | |
| 系统架构：一级功能 | 应用架构：一级应用功能 | 遵从说明 |
| *电量电费* | *电费管理* | *细化* |
|  |  |  |

配图简述应用架构

### 3.4.3数据架构

*【编写说明】描述本系统架构对数据架构的遵从情况。此章节平台类型系统可裁剪。*

*“数据域”和“数据主题”应引用总体架构蓝图数据架构部分，如蓝图规划中没有相应设计，应遵循架构资产修编流程，提出架构资产修编申请。*

*“系统架构：数据实体”需逐一列出系统涉及到的业务数据实体；“数据架构：数据实体”需参考总体数据架构蓝图资产，列出对应的数据实体；“遵从说明”描述系统数据实体与总体数据架构数据实体的遵从关系，可选项为：遵从、细化、参照（总体数据架构中没有对应项）。*

表 数据架构遵从对照

|  |  |  |
| --- | --- | --- |
| 数据域 | *人力资源管理* | |
| 数据主题 | *员工* | |
| 系统架构：数据实体 | 数据架构：数据实体 | 遵从说明 |
| *学员* | *员工* | *细化* |
|  |  |  |

### 3.4.4技术架构

*【编写说明】描述本系统架构对技术架构的遵从情况。*

*“总体架构：系统名称”应引用总体架构蓝图技术架构部分，如蓝图规划中没有相应设计，应遵循架构资产修编流程，提出架构资产修编申请。*

*配图简述技术架构*

表 技术架构遵从对照

|  |  |  |
| --- | --- | --- |
| 本系统名称 | 总体架构：系统名称 | 遵从说明 |
| *一体化缴费平台* | *一体化缴费平台* | *遵从* |
| 集成场景 | | |
| 系统架构：集成场景 | 技术架构：集成场景 | 遵从说明 |
| *逐一列出本系统的集成场景* | *总体技术架构蓝图设计资产中对应的集成场景* | *遵从：完全一致*  *细化*  *参照（技术架构无对应集成场景）* |
|  |  |  |
| 产品标准 |  | |
| 系统架构：软件产品 | 技术架构：软件产品 | 遵从说明 |
| *系统拟使用的软件产品（操作系统、数据库、中间件等基础软件）和版本号* | *与之对应的技术架构中定义的软件产品* | *遵从：完全一致*  *参照（技术架构无对应集成架构模式）* |
|  |  |  |

# 4业务能力视图

## 4.1业务目标

*【编写说明】此处的业务功能应与《需求规格说明书》中的业务目标章节保持一致。*

## 4.2组织单元

*【编写说明】此处的业务功能应与《需求规格说明书》中的组织单元章节保持一致。*

## 4.3岗位

*【编写说明】此处的业务功能应与《需求规格说明书》中的岗位章节保持一致。*

## 4.4业务流程

*【编写说明】此处的业务功能应与《需求规格说明书》中的业务流程章节保持一致。*

## 4.5业务活动

*【编写说明】此处的业务功能应与《需求规格说明书》中的业务活动章节保持一致。*

## 4.6业务信息

*【编写说明】此处的业务流程应与《需求规格说明书》中的业务信息章节保持一致。*

# 5功能视图

## 5.1角色定义

*【编写说明】此处的功能视图应与《需求规格说明书》中的角色定义章节保持一致。*

## 5.2功能视图

*【编写说明】此处的功能视图应与《需求规格说明书》中的功能视图章节保持一致。*

## 5.3功能清单

*【编写说明】此处的功能清单应与《需求规格说明书》中的功能清单章节保持一致。*

# 6系统数据视图

## 6.1概念数据模型

*【编写说明】对数据子主题进一步细化，通过概念数据模型设计出顶层概念数据实体。*

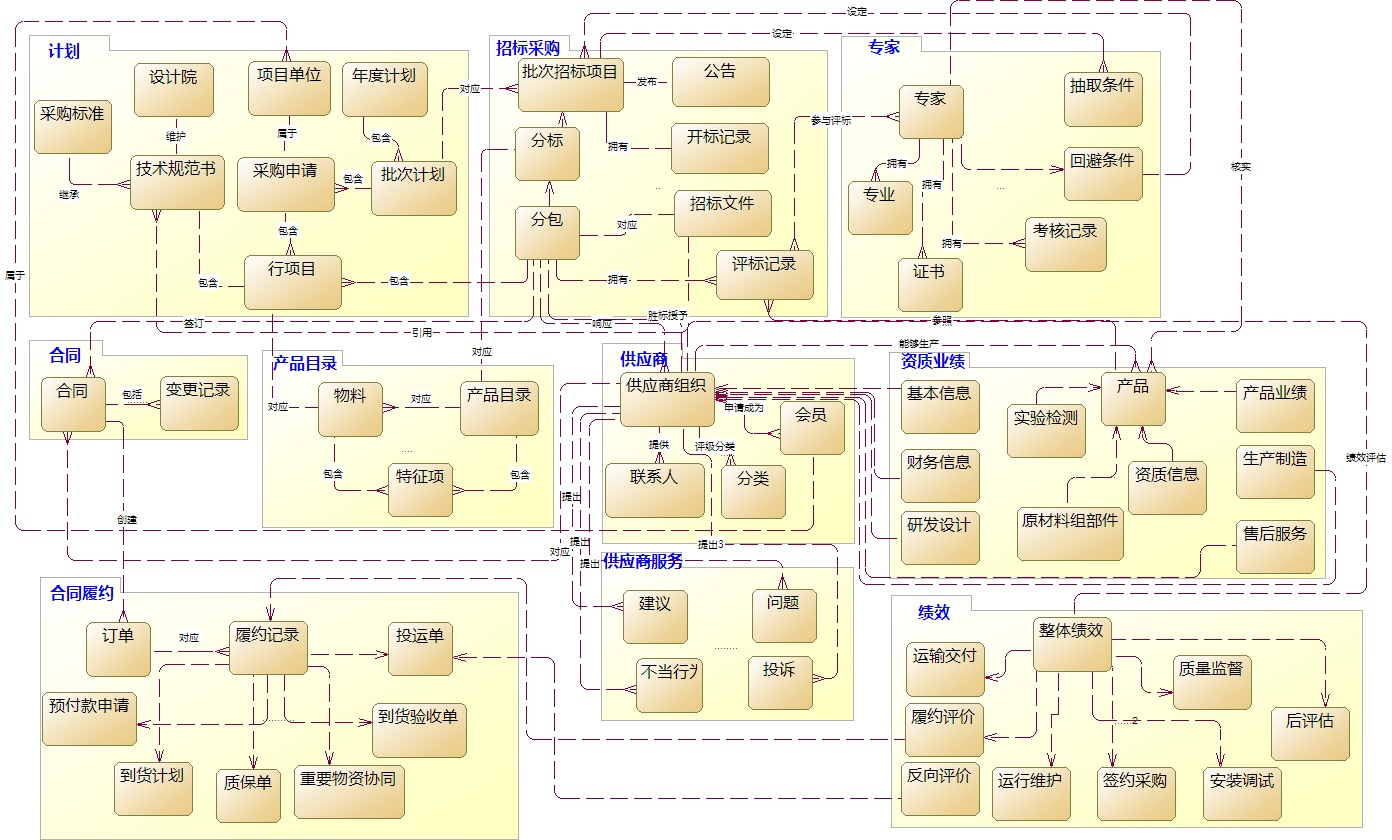


图10 概念数据模型

## 6.2逻辑数据模型

*【编写说明】描述本系统数据实体逻辑模型，包括数据实体间的逻辑关系，数据实体关键数据属性，数据实体键。*

*【示例】*



图11 数据模型

具体的逻辑数据实体定义详见附录[13.2逻辑数据实体分项定义](#_逻辑数据实体分项定义)

## 6.3数据分类

*【编写说明】描述本系统设计数据的分类*

*【示例】*

表 数据分类清单

|  |  |
| --- | --- |
| 数据实体 | 数据描述 |
| *XXX* | *结构化* |
| *Xxx* | *非结构化* |
| *Xxxx* | *主数据* |

## 6.4数据流转

*【编写说明】描述主要数据在本系统及其相关系统的数据流向*

*【示例】*

图12 数据流转图

表 数据流转清单

|  |  |  |
| --- | --- | --- |
| 交换数据实体 | 源系统 | 目标系统 |
| *销售数据* | *CRM* | *ERP* |
| *客户信息* | *CRM* | *ERP* |
| *订单* | *CRM* | *ERP* |
| *订单状态* | *ERP* | *CRM* |
| *账务信息* | *CRM* | *ERP* |
| *合同/协议* | *CRM* | *ERP* |
| *授权* | *ERP* | *CRM* |
| *发票及收付款信息* | *ERP* | *CRM* |
| *绩效数据* | *ERP* | *CRM* |
| *雇员管理* | *CRM* | *ERP* |
| *绩效管理* | *ERP* | *CRM* |
| *知识管理* | *ERP* | *CRM* |
| *培训* | *ERP* | *CRM* |
| *供应商主数据* | *SG-MDM* | *CRM* |
| *产品目录、产品规范* | *PLM* | *CRM* |
| *产品需求、产品预测* | *CRM* | *PLM* |

## 6.5数据存储与分布

*【编写说明】描述本系统相关数据在不同系统的分布以及存储方式。*

*【示例】*

表 数据存储清单

|  |  |
| --- | --- |
| 数据实体 | 存储系统名称 |
| *XXX* | *SG-MDM，营销系统* |
|  |  |

表 数据分布清单

|  |  |  |
| --- | --- | --- |
| 数据实体 | SG-MDM | 营销系统 |
| *XXX* | *O* | *C* |
|  |  |  |

*说明：*

* + - 1. *O-owner；*
      2. *C-copy“SG-MDM”和“营销系统”列对应到数据存储清单表的存储系统名称。*

# 7系统组件视图

*【编写说明】系统的功能由一系列的组件协作实现。而组件是由一组紧密耦合的对象构成，通常用来完成独立的功能。组件类型一般可以分为平台组件、功能组件、公共组件和接口组件。公共组件分为可以重用的功能组件和质量属性相关的组件。*

*系统功能的实现是由承担不同功能的组件协作完成。为清晰界定组件职责和协作通讯方式，实现系统各个组成部分职责清晰和松耦合、高内聚的设计目标，将组件按其职责划分为不同的逻辑层次。*

## 7.1系统逻辑分层

*【编写说明】首先给出系统逻辑分层图，然后按如下表格定义各层设计要素。*

*【注意】*

1. *下列表格要素是必须说明项，不限于下列表格定义的要素；*
2. *各逻辑层可以分章节说明。*

*【示例】*

******

图13 系统逻辑分层图

表 系统逻辑分层说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 逻辑层次 | 职责描述 | 技术实现 | 逻辑层次依赖 | 层间通信 |
| 展现层 | 1. *接受用户输入* 2. *呈现数据* | 1. *使用Flex技术实现动态图表* 2. *使用Flex技术，并结合Web GIS切片实现地图导航* | *依赖应用服务层* | 1. *采用消息在展现层与服务层通信* 2. *层间采用http(s)协议* |

## 7.2组件关联设计

*【编写说明】描述功能组件间、功能组件与公共组件间的关联（依赖）关系。所谓的组件关联（依赖）是指为实现某项系统功能而需要的组件间关系。*

图14 组件关联图

*【注意】如一张图不便描述所有组件关联关系，可以分章节描述。*

表 组件关联清单

|  |  |  |  |
| --- | --- | --- | --- |
| 组件编号-名称 | 组件的方法 | 关联的组件编号-名称 | 关联的组件的方法 |
|  |  |  |  |

## 7.3组件时序设计

*【编写说明】在此章节，对关键的接口组件，分组件绘制时序图，并进行说明。*

## 7.4功能组件设计

*【编写说明】在此章节，首先绘制功能组件图，再按如下表格设计要素定义系统组件设计。*

### 7.4.1组件清单

*【编写说明】如果每层放置的组件很多，可以将每一层作为一个图进行绘制。*



图15 功能组件图

*【编写说明】列出功能组件清单*

表 功能组件清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 功能组件编号-名称 | 功能编号-名称 | 系统逻辑分层 | 包含的组件编号-名称 | 是否接口组件 | 非非功能性要求 |
| 1. *XX-xx功能组件* | 1. *XX-功能1* 2. *XX-功能2* | *展现层* | *XX-xx表单组件1* | *否* | *无* |
| *XX-xx报表组件1* | *否* | *无* |
| *应用层*  *…* | *XX-xx逻辑组件1* | *否* | *无* |
| *XX-xx接口组件2* | *是* | *只能在XX时间段内调用* |

### 7.4.2功能组件分项说明

*详见附录*[13.1.1 功能组件分项说明](#_功能组件分项说明)

## 7.5接口组件设计

*【编写说明】按如下表格定义接口组件设计要素。*

*【注意】*

*如本系统没有设计相关的质量属性组件应予以说明；*

*不限于下面表格中所列的质量属性组件*

### 7.5.1组件清单

*【编写说明】如果每层放置的组件很多，可以将每一层作为一个图进行绘制。*



图16 接口组件图

*列出接口组件清单*

表 接口组件清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 分类 | | 接口组件编号-名称 | 职责描述 | 来源 | 系统逻辑分层 |
| 本系统重用功能组件 | | *XX-xx表单组件1* |  |  |  |
|  |  |  |  |
| 质量属性  组件 | 认证 |  |  |  |  |
| 授权 |  |  |  |  |
| 缓存 |  |  |  |  |
| 异常管理 |  |  |  |  |
| 日志 |  |  |  |  |
| 验证 |  |  |  |  |
| ... | *可扩展* |  |  |  |

### 7.5.2接口组件分项说明

*详见附录*[*13.1.2接口组件分项说明*](#_公共组件分项说明_1)

## 7.6公共组件设计

*【编写说明】公共组件通常可以分为可以重用的功能组件和质量属性相关的公共组件，按如下表格定义公共组件设计要素。*

*【注意】*

*如本系统没有设计相关的质量属性组件应予以说明；*

*不限于下面表格中所列的质量属性组件*

### 7.6.1组件清单

*【编写说明】如果每层放置的组件很多，可以将每一层作为一个图进行绘制。*



图16 公共组件图

*列出公共组件清单*

表 公共组件清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 分类 | | 公共组件编号-名称 | 职责描述 | 来源 | 系统逻辑分层 |
| 本系统重用功能组件 | | *XX-xx表单组件1* |  |  |  |
|  |  |  |  |
| 质量属性  组件 | 认证 |  |  |  |  |
| 授权 |  |  |  |  |
| 缓存 |  |  |  |  |
| 异常管理 |  |  |  |  |
| 日志 |  |  |  |  |
| 验证 |  |  |  |  |
| ... | *可扩展* |  |  |  |

### 7.6.2公共组件分项说明

*详见附录*[*13.1.3公共组件分项说明*](#_公共组件分项说明_1)

# 8系统集成视图

## 8.1总体集成

*【编写说明】采用图形化方式描述系统间集成关系。*

*【示例】*



图17 系统总体集成图

## 8.2集成场景

*【编写说明】按下列表格定义集成场景要素。*

*【示例】*

表 集成场景清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 场景编号 | 场景描述 | | | | | 集成方式 |
| 源系统 | 目标系统 | 频率 | 实时性 | 数据量 |
| *IC001* | *ERP* | *企业门户* | *1-5次/天* | *10ms-100ms* | *20K-1M* | *界面集成* |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## 8.3集成设计

*【编写说明】在此章节，对8.2确定的各集成场景进行设计，按界面集成、应用集成、数据集成分类进行设计。*

*【注意】*

*如实际设计中无对应场景，则明确说明无对应场景。*

### 8.3.1界面集成

*【编写说明】描述界面集成的集成接口组件。*

*【示例】*

*描述界面集成相关的系统和采用的实现技术*

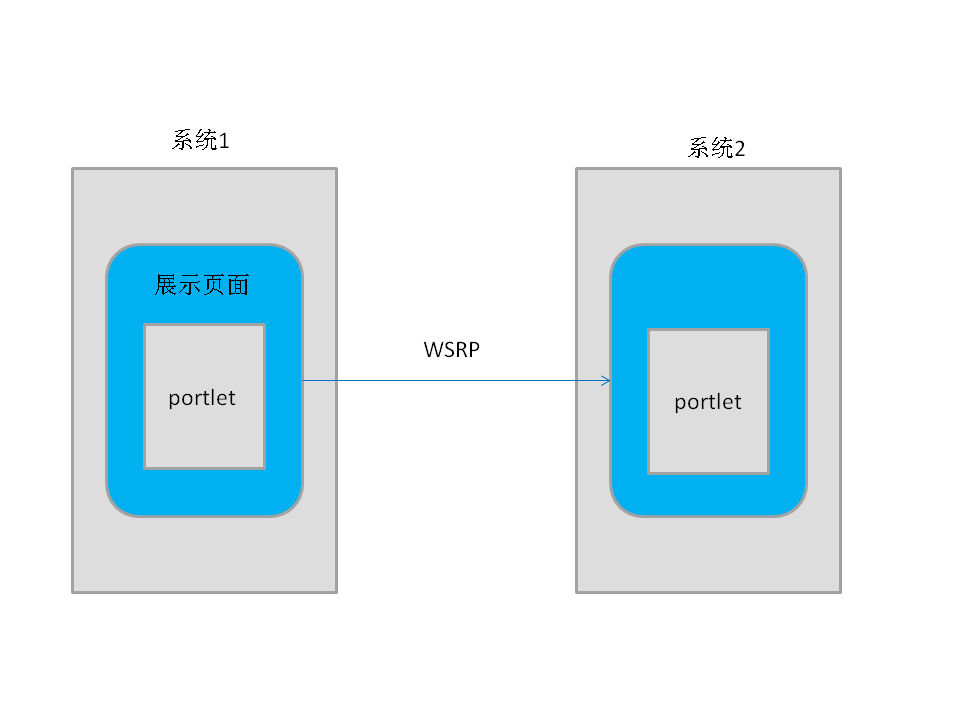


图18 界面集成图

表 界面集成组件定义

|  |  |  |
| --- | --- | --- |
| 集成接口组件编号 |  | |
| 集成接口组件名称 |  | |
| 集成场景编号 |  | |
| 发起方/提供方 | *门户、工作流、应用系统等* | |
| 接口信息 | | |
| 接口名称 | 描述 | 实现技术 |
|  |  | *链接、WSRP等* |

### 8.3.2应用集成

*【编写说明】描述应用集成的集成接口组件。*

*【示例】*

*描述应用集成相关的系统以及采用的集成方式，如果采用集成平台，如采用企业服务总线进行集成，说明总线相关的高阶设计。*

图19 应用集成设计图

表 应用集成设计

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 集成接口组件编号 | | |  | | | | | | |
| 集成接口组件名称 | | |  | | | | | | |
| 集成场景编号 | | |  | | | | | | |
| 发起方/提供方 | | | *发起方为调用其他系统组件，提供方为其他系统调用本组件* | | | | | | |
| 集成方式 | | | *如采用企业服务总线进行集成，或者直连等* | | | | | | |
| 发起方接口信息 | | | | | | | | | |
| 接口名称 | 描述 | 输入消息 | | 输入消息格式 | 输出消息 | 输出消息格式 | 实现技术 | 同步/异步 | 异常处理 |
|  |  |  | | *SOAP/XML/文本* |  | *SOAP/XML/文本* | *JMS/CORBA/Web Service* | *同步调用/同步被调用/异步发送/异步接收* | *重试1次* |
|  |  |  | |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |
| 提供方接口信息 | | | | | | | | | |
| 接口名称 | 描述 | 输入消息 | | 输入消息格式 | 输出消息 | 输出消息格式 | 实现技术 | 同步/异步 | 异常处理 |
|  |  |  | | *SOAP/XML/文本* |  | *SOAP/XML/文本* | *JMS/CORBA/Web Service TODO:举例调整* |  | *重试1次* |
|  |  |  | |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |

### 8.3.3数据集成

*【编写说明】如采用集成接口方式进行数据集成，则集成接口编号和名称应引用“表格23 应用集成设计”中的集成接口编号和名称，否则自行编号。*

*【示例】*

*说明数据集成相关的系统、采用的集成方式，并且给出集成平台的高阶设计。*

图20 数据集成设计图

表 数据集成设计

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 集成接口组件编号 |  | | | |
| 集成接口组件名称 |  | | | |
| 集成场景编号 |  | | | |
| 发起方 |  | | | |
| 发起方数据格式 | *E语言、XML等* | | | |
| 接收方 |  | | | |
| 接收方数据格式 | *E语言、XML等* | | | |
| 集成方式 | *如采用数据交换平台、数据联邦、ETL、ESB* | | | |
| 数据类型 | *结构化数据、空间数据、实时数据等。* | | | |
| 发起方式 | *手动、自动* | | | |
| 时间窗口 | *多久能做完，什么时候做完* | | | |
| 交换数据信息 | | | | |
| 交换数据实体名称 | | 属性 | 数据量 | 校验规则 |
|  | |  |  |  |

# 9系统逻辑部署视图

## 9.1部署单元设计

*【编写说明】定义出系统的所有逻辑部署单元及其依赖关系，并按如下表格要求，说明每个部署单元所包含的组件。*

*【示例】*



图21 部署单元

表 逻辑部署单元定义

|  |  |
| --- | --- |
| 逻辑部署单元编号 | *DU01* |
| 逻辑部署单元名称 | *空间数据部署单元* |
| 功能描述 |  |
| 组件清单 | |
| 组件编号 | 组件名称 |
| *xxx* | *xxx表单组件* |
| *….* | *….* |

## 9.2部署节点设计

*【编写说明】以图形和文字定义部署节点逻辑组成，应描述节点承载的部署单元，并说明设计原因。*

*【示例】*



图22 部署节点

*虚框表示逻辑部署节点，实框表示物理部署节点*

# 10系统物理部署视图

## 10.1部署拓扑

*【编写说明】定义系统硬件网络拓扑结构。*

*【示例】*

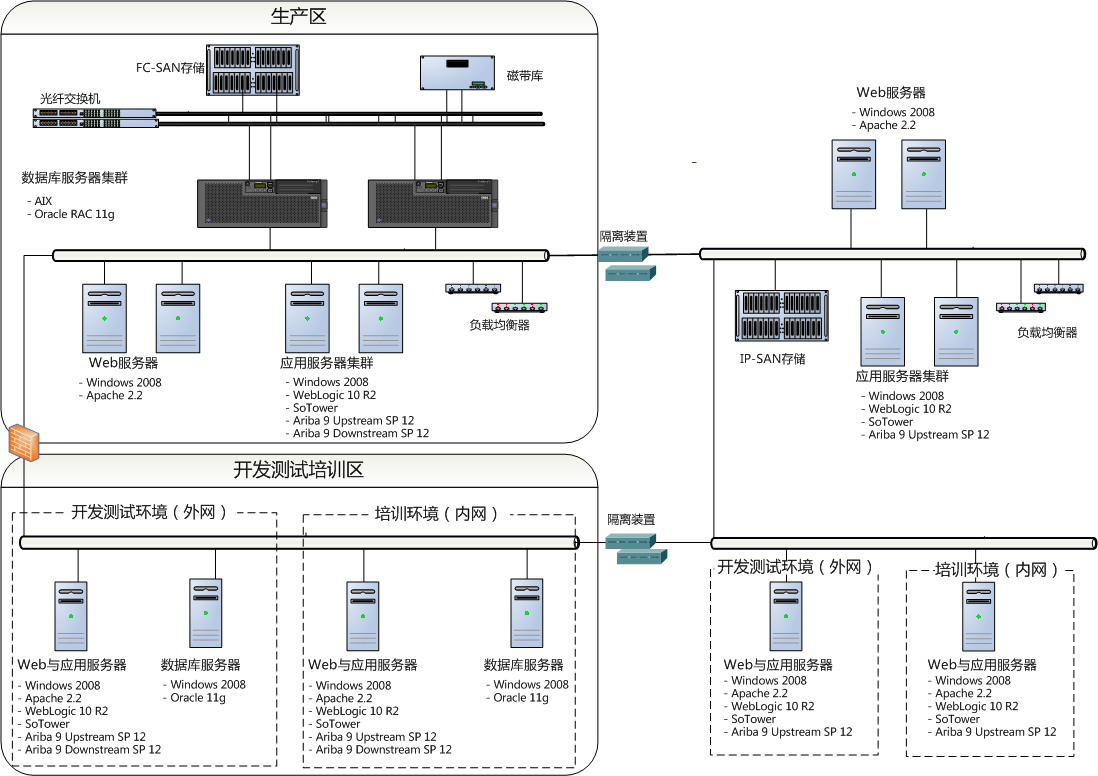


图23 物理部署视图

## 10.2容量规划

*【编写说明】定义硬件容量规划。*

*【注意】*

*遵循《国家电网公司软硬件目标架构设计规范》要求设计硬件环境。*

## 10.3硬件环境设计

*【编写说明】定义执行环境硬件配置。*

*【示例】*

*物理视图硬件清单如下：*

表 物理部署视图硬件清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 物理部署节点编号-名称 | 硬件 | 配置 | 位置 | 备注 |
| *PND05-数据库服务器部署节点* | *数据库服务器* | *1台小型机*  *CPU：2核 1.6 GHz以上*  *内存：4G*  *网卡：2×100/1000M以太网卡*  *操作系统：LINUX*  *数据库：Oracle* | *xx省公司信息管理大区* |  |
| *PND03-应用服务器部署节点* | *应用服务器* | *1台PC服务器*  *CPU：2核 2.40GHz以上*  *内存：4G*  *硬盘：60G*  *网卡：2×100/1000M以太网卡*  *操作系统：Linux* |  |  |
| *PND01-Web服务器部署节点* | *Web服务器* | *PC机*  *CPU：1核 2.40GHz以上*  *内存：1G*  *硬盘：40G*  *网卡：1×100/1000M以太网卡*  *显示器分辨率：1024 x 768*  *操作系统：WindowsXP* |  |  |

## 10.4软件环境设计

*【编写说明】定义执行环境软件配置。*

*【示例】*

*物理视图软件清单示例：*

表 物理部署视图软件清单

|  |  |  |  |
| --- | --- | --- | --- |
| 物理部署节点编号-名称 | 软件名称 | 版本 | 备注 |
| *PND05-数据库服务器* | *操作系统* | *HP-UX B.11.23(ia64)及以上（建议采用可以采用11.31版本）* |  |
| *数据库* | *Oracle10g* |  |
| *PND06-应用服务器* | *操作系统* | *HP-UX B.11.23(ia64)及以上（建议采用可以采用11.31版本）* |  |
| *应用服务器* | *WebSphere 7.0* |  |
|  | *…* | *…* |  |

# 11系统灾备视图

*【编写说明】对于明确要求采用应用级灾备的系统，需另行编写《应用级灾备子方案》,否则按本模板编写数据级灾备设计。*

## 11.1关键技术选择

*【编写说明】根据系统数据保护时间要求和数据特点，选取合适的数据级灾备复制技术。*

*【注意】从国网数据级灾备已选用的数据库复制和存储复制之中选择其一，对于结构化数据库优先采用数据库复制，对于非结构化数据和应用数据采用存储复制*

## 11.2灾备策略设计

*【编写说明】根据灾备保护策略的选择（例如灾备端与生产端选择软硬件资源同级配置或降级配置，灾备端与生产端选择软硬件资源同构或异构等），设计灾备系统的数据保护和数据恢复能力。*

*【示例】*

*1）现有生产中心业务系统与灾备中心相关灾备系统的设备类型和操作系统版本应保持一致。*

*2）灾备中心的处理能力将优先考虑满足数据级灾备复制的最低需求。其中：数据库复制主机按照2CPU、8G内存进行配置，验证区主机按照典型网省的典型系统主机进行配置。*

*3）灾备主机的HBA卡按照不同应用，独立访问端口的设计，确保性能不降低。*

*4）灾备存储容量和生产保持一致，存储容量要有一定的冗余以支持演练。*

*5）灾备中心数据按照不同层级存储，参考目标架构对不同业务系统数据的分类及存储要求，在灾备中心完全按照目标架构的规范进行数据的分级存储。*

*6）灾备中心存储磁盘RAID配置以等同于或者略低于生产中心标准配置。*

*7）存储空间配置要考虑验证和演练的需求。*

*8）数据复制网络和日常运维管理网络单独设计。*

## 11.3灾备架构设计

*【编写说明】通过系统数据级灾备架构图，展示被灾备的系统名称、选用的关键技术、灾备复制策略、数据存储策略、传输路径等主要信息。*

*【示例】*

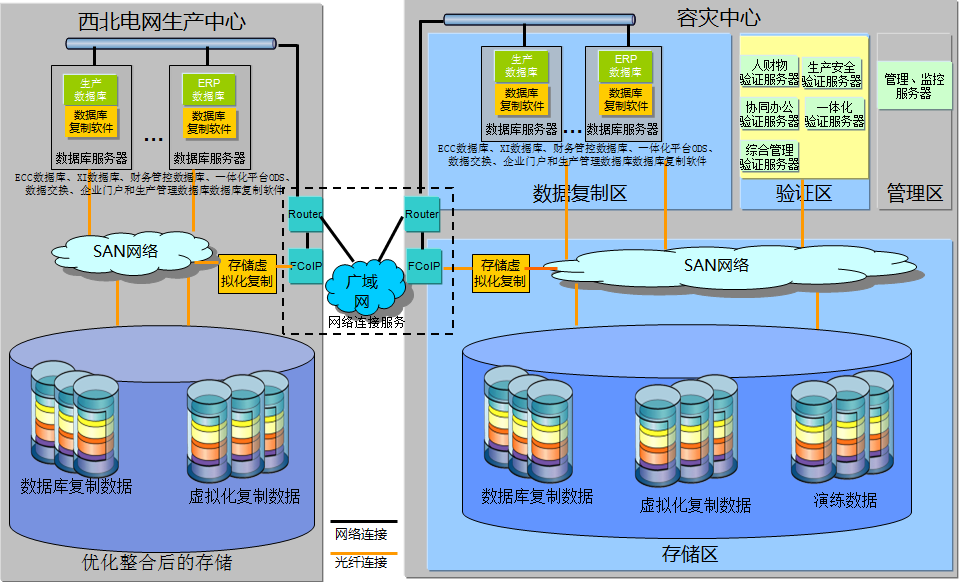


图24 灾备逻辑架构视图

## 11.4灾备设备配置

*【编写说明】根据数据级灾备架构设计定义灾备环境软硬件配置。*

*【示例】*

*灾备端硬件清单如下：*

表 灾备端硬件清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 描述 | 硬件 | 配置 | 位置 | 备注 |
| *XX省营销生产库数据库复* | *数据库服务器*  *外置高端存储* | *配置为4C/16G/300GB\*2 /HBA\*2/光纤网卡\*2/电口网口1个*  *操作系统AIX5.3*  *外置高端存储 5000GB* | *北京灾备中心* |  |
| *XX省营销管理库数据库复制* | *数据库服务器*  *外置高端存储* | *配置为4C/16G/300GB\*2 /HBA\*2/光纤网卡\*2/电口网口1个*  *操作系统AIX5.3*  *外置高端存储 5000GB* | *北京灾备中心* |  |
| *XX省营销文档库存储复制* | *外置高端存储*  *FCOIP设备* | *外置高端存储 300GB*  *FCOIP设备2台，每台4个FC接口,2个以太网电口及license* | *北京灾备中心* |  |

表 灾备端软件清单

|  |  |  |  |
| --- | --- | --- | --- |
| 软件名称 | 版本 | 数量 | 备注 |
| *数据库复制软件* | *OGG11.2* | *20C* |  |
| *数据库* | *Oracle10g* | *20C* |  |
| *存储复制许可* |  | *300GB* |  |
| *…* | *…* |  |  |

# 12系统安全视图

*【编写说明】*

*所有系统均需填写本章节内容。对于信息安全保护等级在三级（含）以上系统或者对外提供服务的系统，还需单独编写附录13.3章节系统安全设计方案。*

## 12.1总体安全视图

*【编写说明】*

*描述系统安全防护等级、总体安全防护目标，并配备系统安全防护技术架构或部署图。*

*【示例】*

*95598智能互动网站等级保护初定为三级，其安全防护依据《国家电网公司智能电网信息安全防护总体方案》（国家电网信息〔2011〕1727号）要求，遵循“分区分域、安全接入、动态感知、全面防护”的安全策略，按照等级保护三级系统要求进行安全防护设计，并根据业务系统的不断完善加强对网站的防护，最大限度的保障95598智能互动网站的安全、可靠和稳定运行。安全防护总体技术架构如下图所示：*



图25系统安全防护总体技术架构

*防护目标：*

*1. 保障95598智能互动网站用户身份真实可信，防止恶意用户、非授权用户访问；*

*2. 保障用户传输及交互数据的完整性、保密性：防范外网用户访问信息外网应用服务器时数据被窃听、篡改。防范敏感信息如用户口令密码、业务数据被泄露；*

*3. 保障95598智能互动网站应用系统的安全性，防止对网站应用系统资源的非授权访问、敏感数据泄漏以及对系统非法攻击等。*

## 12.2应用安全

*【编写说明】描述应用安全设计*

*【示例】*

表 应用安全设计清单

|  |  |
| --- | --- |
| 控制点 | 防护策略设计 |
| *身份认证* | *设置密码的存储和传输安全；*  *保护身份验证Cookie；*  *同一用户同时只允许登录一个；* |
| *授权* | *设计资源访问控制方案，验证用户访问权限；*  *限制用户对系统级资源的访问；*  *设计统一的访问控制机制；* |
| *输入输出验证* | *设计验证所有来源不在可信范围之内的输入数据；*  *应在服务器端和客户端都应进行输入验证；*  *应对输入内容进行规范化处理后再进行验证，如文件路径、 URL地址等，*  *需要规范化为标准的格式后再进行验证；*  *应当从服务器端提取关键参数，禁止从客户端输入；* |
| *配置管理* | *确保配置存储的安全；*  *应使用最少特权进程和服务帐户；*  *应避免应用程序调用支撑系统资源；*  *单独分配管理特权；* |
| *会话管理* | *设计登录成功使用新的会话；*  *设计会话数据的存储安全；*  *设计会话数据的传输安全；*  *设计会话的安全终止；*  *设计合理的会话存活时间；* |
| *加密技术* | *不使用自创加密方法；*  *确保加密密钥的安全；* |
| *参数操作* | *不要信任 HTTP 头信息；*  *确保用户没有绕过检查；*  *应验证从客户端发送的所有数据；* |
| *异常管理* | *使用结构化异常处理机制；*  *使用通用错误信息；*  *程序发生异常时，应终止当前业务，并对当前业务进行回滚操作，保*  *证业务的完整性和有效性，必要时可以注销当前用户会话；*  *程序发生异常时，应在日志中记录详细的错误消息；* |
| *审核和日志* | *日志记录事件应至少包含以下事件：*  *审计功能的启动和关闭；*  *应用系统的启动和停止；*  *配置变化；*  *访问控制信息；*  *用户对数据的异常操作事件* |

## 12.2数据安全

*【编写说明】描述数据安全设计*

*【示例】*

表 数据安全设计清单

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **数据安全属性分析** | | | | | | | | | | |
| 数据类别 |  | | 使用者说明 | |  | | | | | |
| 机密性赋值 |  | | 完整性赋值 | |  | | | 可用性赋值 |  | |
| **数据流转分析** | | | | | | | | | | |
| 数据流转过程  简要说明 | *描述数据的来源，由谁使用，使用过程中途径哪些系统环节* | | | | | | | | | |
| 是否在用户端呈现 | | *是/否* | | 是否用户端保存 | | *是/否* | 是否在网络中传输 | | | *是/否* |
| 是否经过可信与不可信边界传输 | | *是/否* | | 是否通过无线网络传输 | | *是/否* | 是否在应用系统间传输 | | | *是/否* |
| 是否保存在应用系统中 | | *是/否* | |  | |  |  | | |  |

## 12.3主机安全

*【编写说明】制定主机安全防护措施。*

*【示例】*

表 主机安全设计清单

|  |
| --- |
| 系统主机描述 |
| *描述本项目中所使用主机的功能。* |
| 主机安全设计 |
| *根据等级保护和智能电网安全防护方案的要求从主机访问控制、主机安全加固、主机入侵检测、主机内容安全、病毒防范、主机身份鉴别、数据加密、主机监控审计、备份恢复、资源控制、剩余信息保护这几个方面给出主机安全详细设计。* |

## 12.4网络安全

*【编写说明】制定网络安全防护措施。*

*【示例】*

表 网络安全设计清单

|  |
| --- |
| 系统网络环境描述 |
| *描述本项目中的实际网络环境。* |
| 网络安全设计 |
| *根据等级保护和智能电网安全防护方案的要求从网络设备安全、网络基础服务安全 、网络业务信息流安全和无线安全几个方面给出网络安全设计的具体措施。* |

## 12.5终端安全

*【编写说明】制定终端安全防护措施。*

*【示例】*

表 终端安全设计清单

|  |
| --- |
| 系统终端类型描述 |
| *描述终端具体类型：包括信息内外网办公计算机终端、移动作业和移动办公终端和信息采集类终端。* |
| 终端安全设计 |
| *根据等级保护和智能电网安全防护方案的要求根据具体终端的类型、应用环境以及通信方式等设计适宜的防护措施。* |

## 12.6其他

*【编写说明】编写其他安全方面的策略。*

# 13系统交互视图

## 13.1界面框架设计

*【编写说明】设计系统登录页、首页、各业务场景界面框架。*

*【示例】*



## 13.2系统控件选择

*【编写说明】根据业务场景与功能，选取合适的界面控件。*

*【示例】*

表 系统控件清单

|  |  |  |  |
| --- | --- | --- | --- |
| 业务场景 | 功能页面名称 | 选择控件 | 控件用途 |
| *业务代办* | *首页代办页面* | *表格控件* | *通过表格控件，以列表形式展示单据序号、单据状态、单据号单据类型、提交时间、单据金额、单据事由。其中单据状态、单据类型支持筛选，提交时间、单据金额支持排序功能。* |
| *业务代办* | *首页代办页面* | *复选框控件* | *通过复选框供用户选择是通过列表形式查看代办单据或者是通过视窗形式查看代办单据。* |
| *。。。* | *。。。* | *。。。* | *。。。* |

# 14附录

## 14.1系统组件视图

### 14.1.1[功能组件分项说明](#_功能组件分项说明_1)

*【编写说明】描述功能组件方法的相关内容*

表 XX-xx表单组件1

|  |  |  |  |
| --- | --- | --- | --- |
| 方法名称 | 描述 | 输入数据实体 | 输出数据实体 |
| *XXX* | *XXX* |  |  |
|  |  |  |  |
|  |  |  |  |

表 XX-xx表单组件2

|  |  |  |  |
| --- | --- | --- | --- |
| 方法名称 | 描述 | 输入数据实体 | 输出数据实体 |
| *XXX* | *XXX* |  |  |
|  |  |  |  |
|  |  |  |  |

### 14.1.2[接口组件分项说明](#_公共组件分项说明)

*【编写说明】描述接口组件方法的相关内容*

表 接口组件方法清单

|  |  |
| --- | --- |
| 方法名称 | 描述 |
| *XXX* | *XXX* |
|  |  |
|  |  |

### 14.1.3[公共组件分项说明](#_公共组件分项说明)

*【编写说明】描述公共组件方法的相关内容*

表 公共组件方法清单

|  |  |
| --- | --- |
| 方法名称 | 描述 |
| *XXX* | *XXX* |
|  |  |
|  |  |

## 14.2[逻辑数据实体分项定义](#_逻辑数据模型)

表 逻辑数据实体定义表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编号-名称 | *XXX-单位信息* | | | | |
| 所属数据域 |  | | | | |
| 所属数据主题 |  | | | | |
| 是否主数据 | *是* | | | | |
| 代码 | *HrOrgUnit* | | | | |
| 与其他实体关系 |  | | | | |
| 备注 |  | | | | |
| 字段名称 | 字段代码 | 数据类型 | 数据长度 | 数据精度 | 主键/外键 |
| 单位代码 | *deptCode* | *VARCHAR* | *30* |  | *主键* |
| 单位简称 | *orgShortName* | *VARCHAR* | *255* |  |  |

## 14.3系统安全设计子方案

*【编写说明】对于信息安全保护等级在三级（含）以上系统或者对外提供服务的系统，需单独编写本章节专项安全设计子方案。二级系统或纯内网应用系统，无需编写本章内容。*

*可参照《信息系统全生命周期安全管控之安全设计规范》进行编写。*

### 14.3.1总体安全视图

*【编写说明】*

*描述系统总体安全防护目标并以系统安全防护总体技术架构图辅助说明。*

*【示例】*

*95598智能互动网站等级保护初定为三级，其安全防护依据《国家电网公司智能电网信息安全防护总体方案》（国家电网信息〔2011〕1727号）要求，遵循“分区分域、安全接入、动态感知、全面防护”的安全策略，按照等级保护三级系统要求进行安全防护设计，并根据业务系统的不断完善加强对网站的防护，最大限度的保障95598智能互动网站的安全、可靠和稳定运行。安全防护总体技术架构如下图所示：*



图26 系统安全防护总体技术架构

*防护目标：*

*1. 保障95598智能互动网站用户身份真实可信，防止恶意用户、非授权用户访问；*

*2. 保障用户传输及交互数据的完整性、保密性：防范外网用户访问信息外网应用服务器时数据被窃听、篡改。防范敏感信息如用户口令密码、业务数据被泄露；*

*3. 保障95598智能互动网站应用系统的安全性，防止对网站应用系统资源的非授权访问、敏感数据泄漏以及对系统非法攻击等。*

### 14.3.2边界安全

*【编写说明】*

*说明系统存在哪几类边界及其对应的安全防护措施，以图示的方式显示存在哪几类边界。*

*【示例】*

*95598智能互动网站边界可分为五类：信息外网第三方边界、信息外网横向域边界、信息内外网边界、信息内网纵向安全边界和信息内网横向域间边界。然后针对每一类边界提出安全防护措施。*



图3 系统边界

#### 14.3.2.1第三方边界安全防护

*【示例】*

|  |  |  |
| --- | --- | --- |
| 边界类型 | 边界描述 | 安全控制措施 |
| 信息外网第三方边界 | 信息外网与互联网的边界 | 1. 部署防火墙（互联网边界防火墙和信息外网边界防火墙），实施访问控制，在网络边界对跨越边界传输的信息进行内容过滤，应对应用层数据流进行有效的监视和控制；防火墙登录应使用两种以上鉴别技术的组合实现身份鉴别。 2. 采用入侵检测系统对流经边界的信息流进行入侵检测，基于对外提供的服务类别（如HTTP、DNS等）进行入侵防护； 3. 对于跨越互联网边界所提供的对外服务，应强化访问控制，限制由应用服务器发起的外发连接，在IP地址、协议、端口等层次细化访问控制策略； 4. 采用专用的防DoS/DDoS攻击系统或在防火墙等边界防护设备上采用技术手段防止DoS/DDoS攻击； 5. 应对各类用户和互联网终端与公司信息外网之间进行安全数据交互提供多种身份认证、消息验证、内容过滤、行为审计等机制； 6. 对重要用户提供多种认证措施，并对各种访问及操作行为进行鉴别，对恶意代码进行过滤，阻截恶意信息传入，防止敏感数据泄漏，保障对外服务安全。 7. 应能检测到非授权设备私自外联并能准确定位、阻断。 |

#### 14.3.2.2信息内外网边界安全防护

|  |  |  |
| --- | --- | --- |
| 边界类型 | 边界描述 | 安全控制措施 |
|  |  |  |

#### 14.3.3.3信息内网纵向边界安全防护

|  |  |  |
| --- | --- | --- |
| 边界类型 | 边界描述 | 安全控制措施 |
|  |  |  |

#### 14.3.3.4横向域间边界安全防护

|  |  |  |
| --- | --- | --- |
| 边界类型 | 边界描述 | 安全控制措施 |
|  |  |  |

### 14.3.3应用安全

*【编写说明】*

*应用安全设计包括身份认证、授权、输入输出验证、配置管理、会话管理、加密技术、参数操作、异常管理、日志及审计等十个方面内容。*

*每项安全设计内容参考《信息系统应用安全系列标准 第2部分：安全设计》编写。*

#### 14.3.3.1身份认证

*【示例】*

*1、身份认证方式如下：*

*1）用户名、口令认证。*

*2）一次性口令、动态口令认证。*

*3）证书认证。*

*2、密码的存储和传输安全策略设计：*

*1）禁止明文传输用户登录信息及身份凭证。*

*2）禁止在数据库或文件系统中明文存储用户密码。*

*3）禁止在COOKIE中保存用户密码。*

*4）采用单向散列值在数据库中存储用户密码，并使用强密码，在生成单向散列值过程中加入随机值。*

#### 14.3.3.2授权

#### 14.3.3.3输入输出验证

#### 14.3.3.4配置管理

#### 14.3.3.5会话管理

#### 14.3.3.6加密技术

#### 14.3.3.7参数操作

#### 14.3.3.8异常管理

#### 14.3.3.9日志与审计

#### 14.3.3.10应用交互安全

### 14.3.4数据安全

*【编写说明】从数据安全模型的机密性、完整新和可用性方面开展设计。具体安全设计要求参考《信息系统应用安全系列标准 第2部分：安全设计》编写。*

#### 14.3.4.1数据机密性安全设计

*【示例】*

*1、数据传输保密性设计*

*1）使用加密技术对传输的敏感信息进行机密性保护。*

*2）使用安全的传输协议（如：HTTPS、SFTP等加密传输协议）来传输文件。*

*3）通过加密和数据签名等方式保障客户端和服务器通信的安全性。*

*2、数据使用保密性设计*

*3、数据删除保密性设计*

#### 14.3.4.2数据完整性安全设计

#### 14.3.4.3数据可用性安全设计

### 14.3.5主机安全

*【编写说明】制定主机安全防护措施。*

*主机安全设计应符合GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求、Q/GDW 594-2011 国家电网公司信息化“SG186”工程安全防护总体方案的要求和国家电网公司智能电网信息安全防护能力的要求。*

*根据要求从主机访问控制、主机安全加固、主机入侵检测、主机内容安全、病毒防范、主机身份鉴别、数据加密、主机监控审计、备份恢复、资源控制、剩余信息保护这几个方面给出主机安全详细设计。*

#### 14.3.5.1操作系统安全防护设计

【示例】

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
| 主机病毒防护 | 应当在服务器上部署网络版防病毒软件客户端或服务器版专用防病毒系统。 |
| 数据备份 | 应当定期对操作系统及运行于操作系统之上的业务应用系统、数据库系统进行备份，并定期或在操作环境发生变更时进行备份恢复测试。 |
|  |  |
|  |  |
|  |  |

#### 14.3.5.2数据库安全防护设计

【示例】

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
| 账号管理 | 1、应限制具备数据库超级管理员（SYSDBA）权限的用户远程登录；  2、在数据库权限配置能力内，应根据用户的业务需要，配置其所需的最小权限；  3、应使用数据库角色（ROLE）来管理对象的权限。 |
|  |  |
|  |  |
|  |  |
|  |  |

### 14.3.6网络安全

*【编写说明】制定网络安全设计措施。*

*网络安全设计应符合GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求、Q/GDW 594-2011 国家电网公司信息化“SG186”工程安全防护总体方案的要求和国家电网公司智能电网信息安全防护能力的要求。*

*根据要求从网络设备安全、网络基础服务安全 、网络传输安全几个方面给出网络安全设计的具体措施。*

#### 14.3.6.1网络设备安全

*【示例】*

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
| 设备安全管理 | 1、实现设备安全管理，主要包括以下安全控制措施：  2、本地或远程进行设备管理必须进行身份认证；  3、应制定设备管理策略，包括限定管理IP地址、制定登录超时及帐号锁定策略；  4、应采用较为安全的SSH、HTTPS进行远程管理；  5、 如基于SNMP协议进行网络监控及管理，建议使用SNMP V3版本，Community不应使用Public、Private等默认字段。 |

#### 14.3.6.2网络基础服务安全

*【示例】*

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
|  |  |

#### 14.3.6.3网络传输安全

*【示例】*

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
|  |  |

### 14.3.7终端安全

*【编写说明】制定终端安全防护措施。*

*终端安全设计应符合GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求、Q/GDW 594-2011 国家电网公司信息化“SG186”工程安全防护总体方案的要求和国家电网公司智能电网信息安全防护能力的要求。*

*根据终端类型，将终端分为办公计算机终端、移动作业终端、信息采集类终端、内网控制类等，应针对具体终端的类型、应用环境以及通信方式等制定适宜的终端防护措施；*

#### 14.3.7.1办公计算机终端

【示例】

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
|  |  |

#### 14.3.7.2移动作业终端

*【示例】*

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
|  |  |

#### 14.3.7.3信息采集类终端

*【示例】*

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
|  |  |

#### 14.3.7.4内网控制类终端

*【示例】*

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
|  |  |

#### 14.3.7.5其他终端

*【示例】*

|  |  |
| --- | --- |
| 安全控制措施 | 控制措施实现方式 |
|  |  |